RSAC 2025 Conference

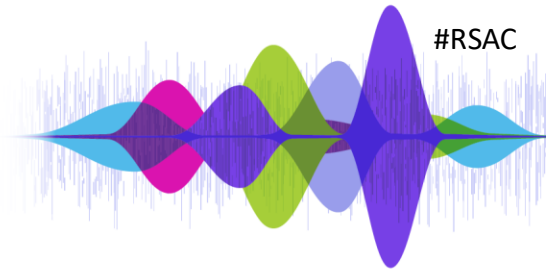
Many Voices.
One Community.

SESSION ID: CLS-W08

Story Time: Attacker Tactics Against Cloud Infrastructure

Shaun McCullough

Instructor | Course Author
SANS SEC541 Cloud Threat Detection sec541.com/rsa2025
www.linkedin.com/in/cybergoof



Disclaimer

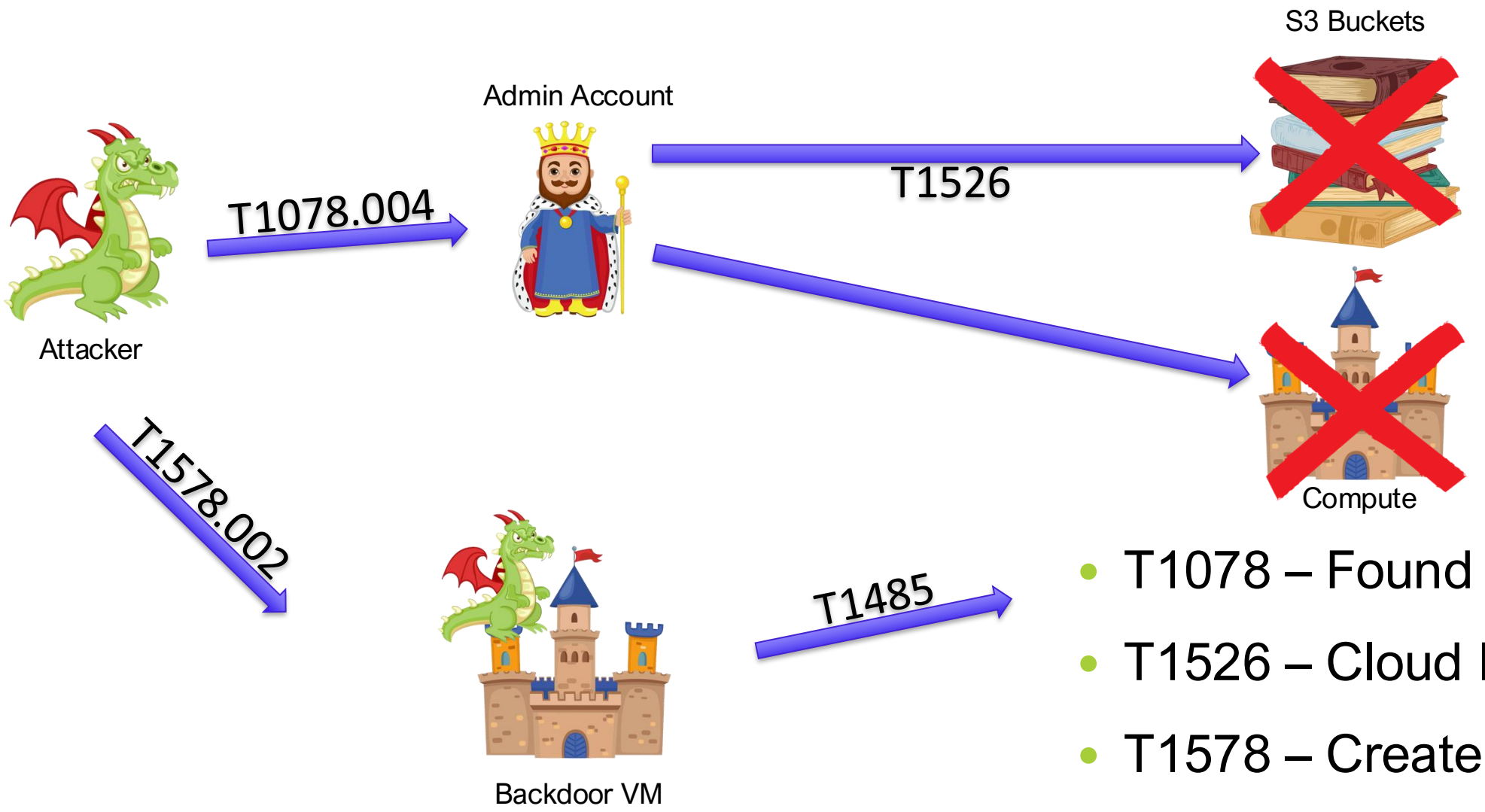
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

The Siege of Code Spaces



- T1078 – Found creds
- T1526 – Cloud Discovery
- T1578 – Create Backdoor
- T1485 – Data Destruction

RSAC 2025 Conference

The Siege of Code Spaces

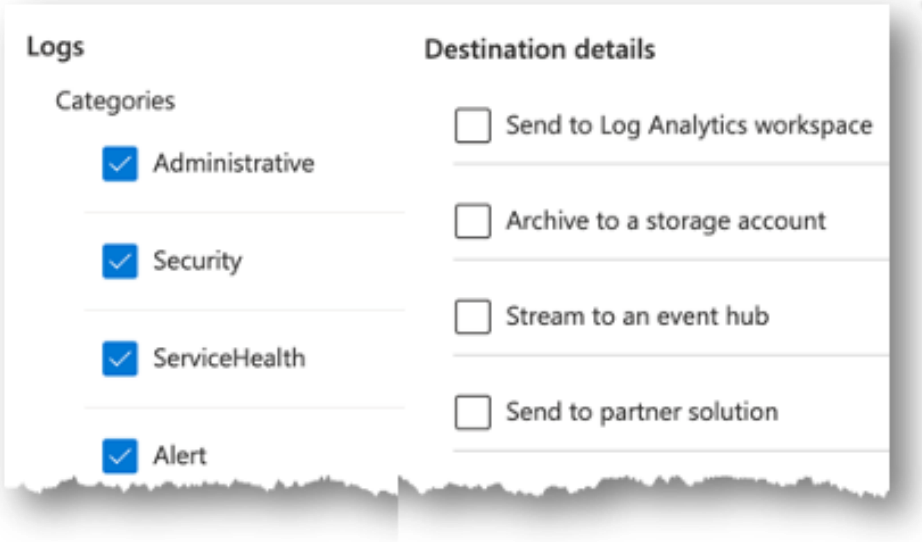
No MFA.

Backups in production = big blast radius

They did not see the backdoor, where are the logs?

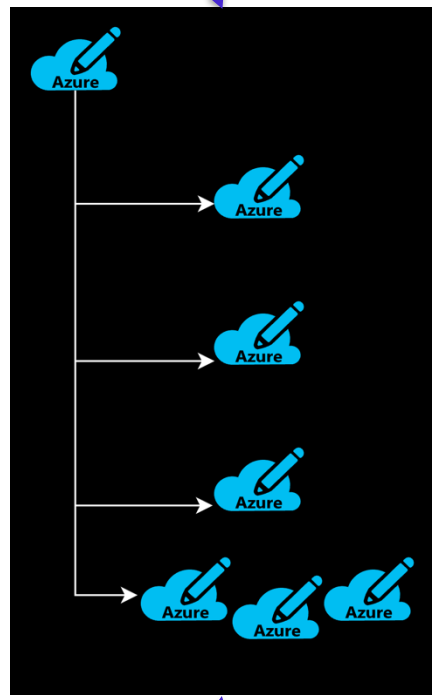
Defense Evasion T1535 – Unused/Unsupported Cloud Regions

Logging in Azure



Diagnostic Settings

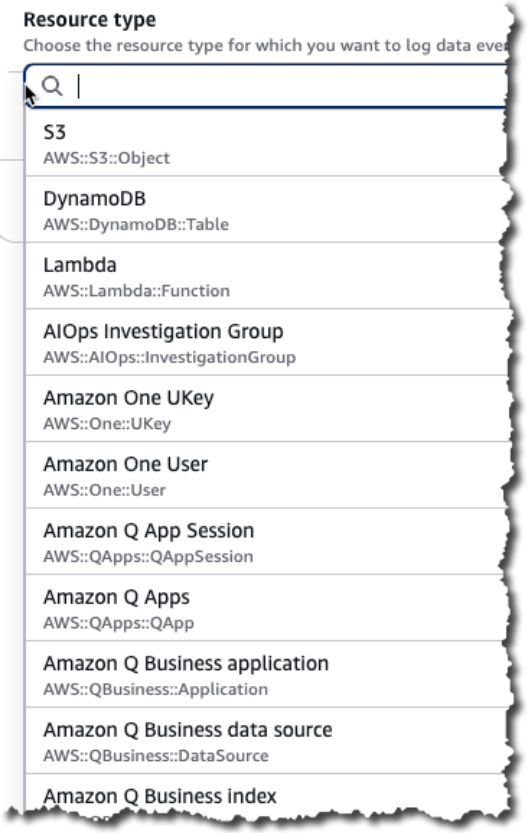
Must apply Diagnostic Settings to EVERY SUBSCRIPTION



Azure Policy

- Audit
- Deny
- Deploy If Not Exist

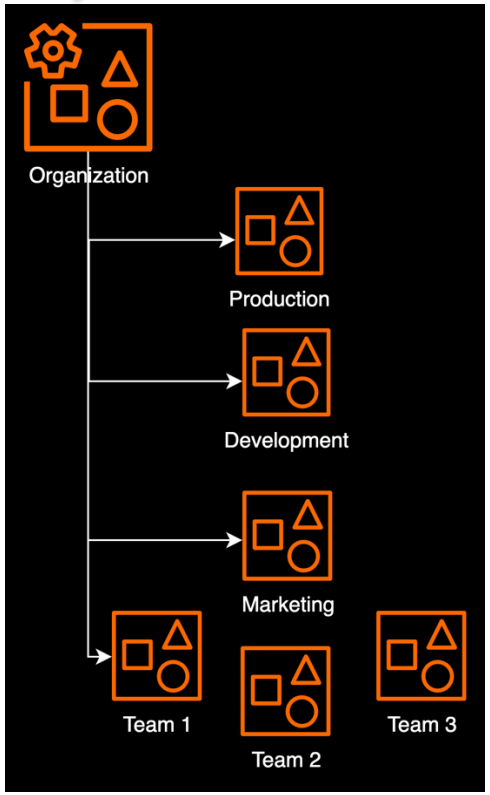
Logging in AWS



CloudTrail

One deployment

covers entire organization.

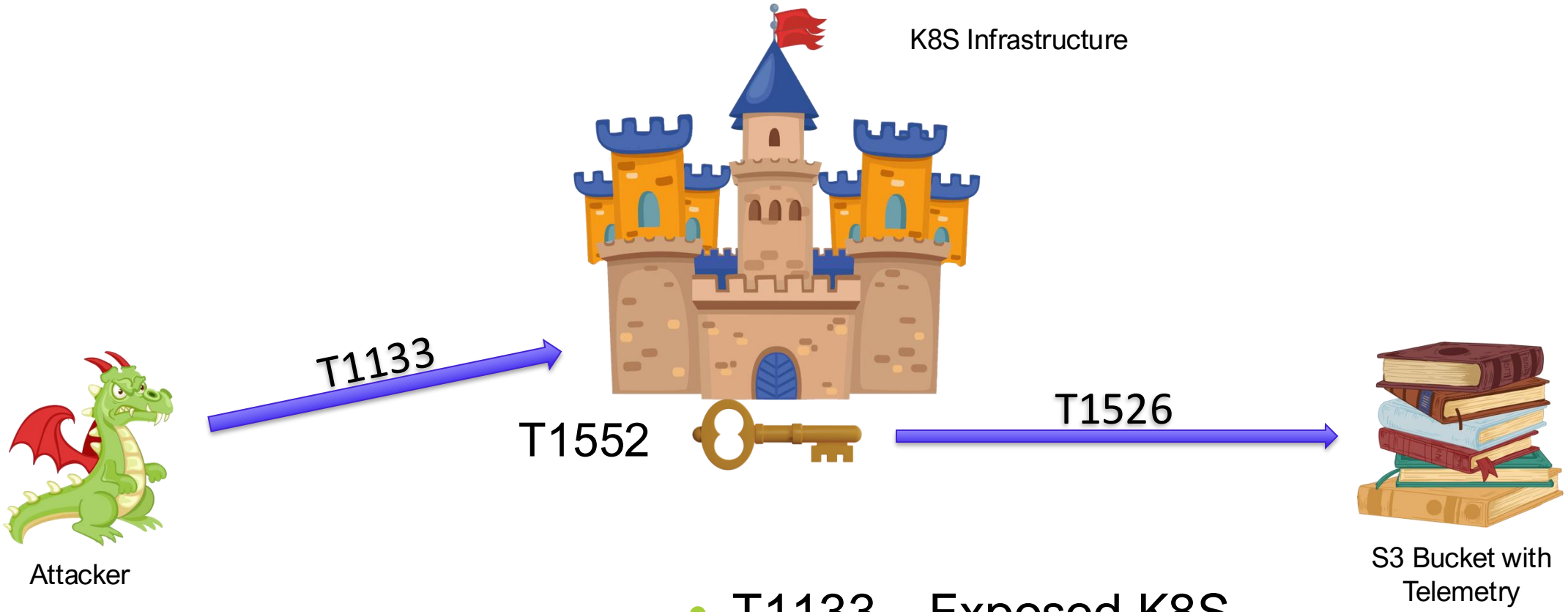


Build it yourself

- Audit
- Deny
- Deploy If Not Exist

RSAC 2025 Conference

Infiltration of Tesla's Kubernetes Fortress



- T1133 – Exposed K8S
- T1552 – Exposed Creds
- T1526 – Discovery
- T1610 – Crypto Miner

Infiltration of Tesla's Kubernetes Fortress

Improve posture management scanning K8S deployments.

Need more control over container image deployment.

Long term credentials are dangerous.

Lateral Movement T1021.007 – Remote Cloud Services

AWS IAM User (Service Accounts)

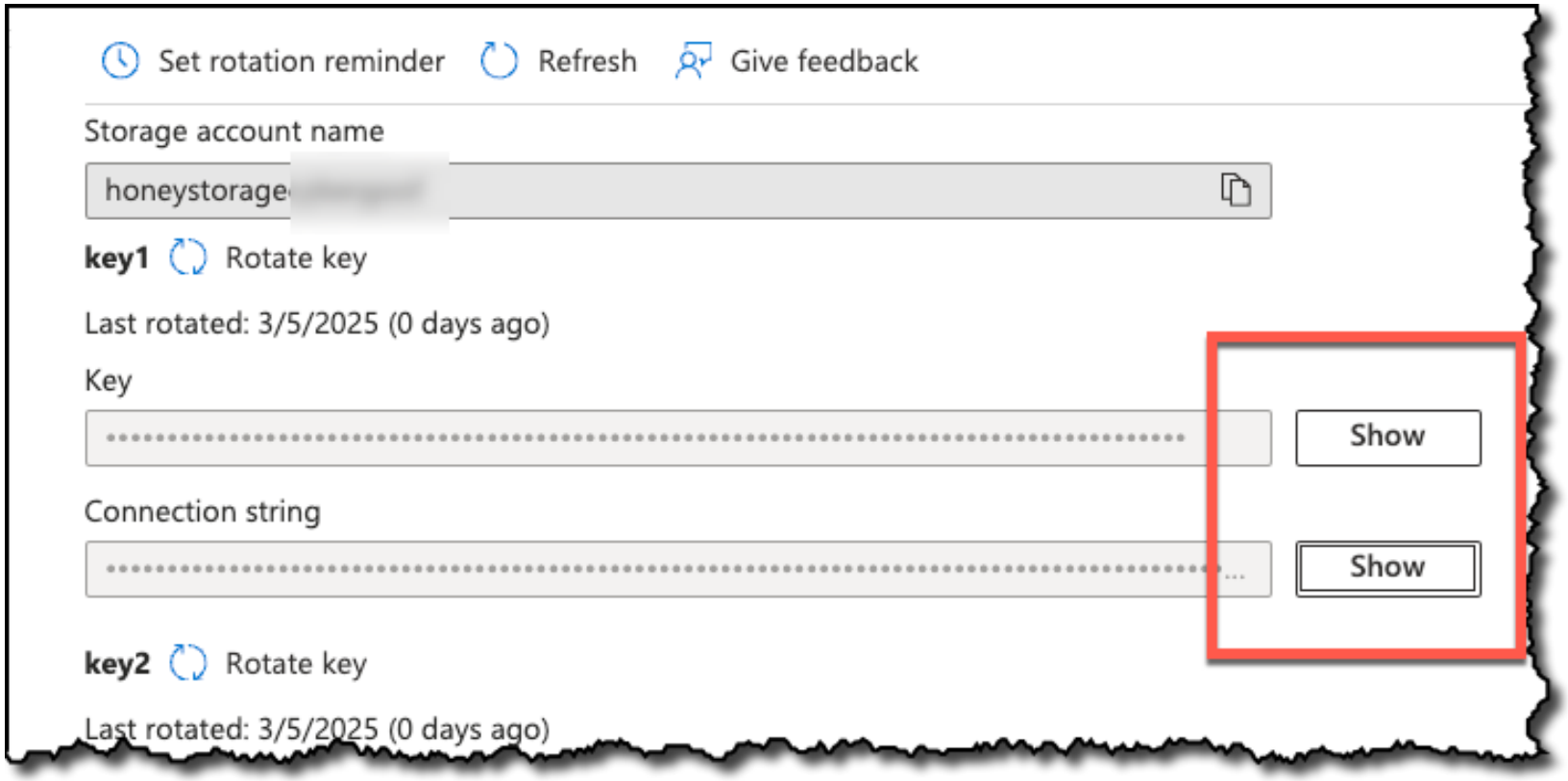
Event name	Event time	Event source	Error code
ListBackupPlans	March 03, 2025,	backup.amazonaws.com	AccessDenied
ListSecrets	March 03, 2025,	secretsmanager.amazonaws.com	AccessDenied
ListDomainNames	March 03, 2025,	es.amazonaws.com	AccessDenied
ListTables	March 03, 2025,	dynamodb.amazonaws.com	AccessDenied
DescribeDBInstances	March 03, 2025,	rds.amazonaws.com	AccessDenied
DescribeInstances	March 03, 2025,	ec2.amazonaws.com	Client Unauthor

- Long term creds
- Anti | Zero Trust
- Usually, over-powered

Get lost all the time

```
"userIdentity": {
    "type": "IAMUser",
    "arn": "arn:aws:iam::                :user/honey_user",
    "accessKeyId": "AKIAYFU23R5YT5CUOB7A",
    "userName": "honey_user"
},
```

Azure Storage Account Access Keys



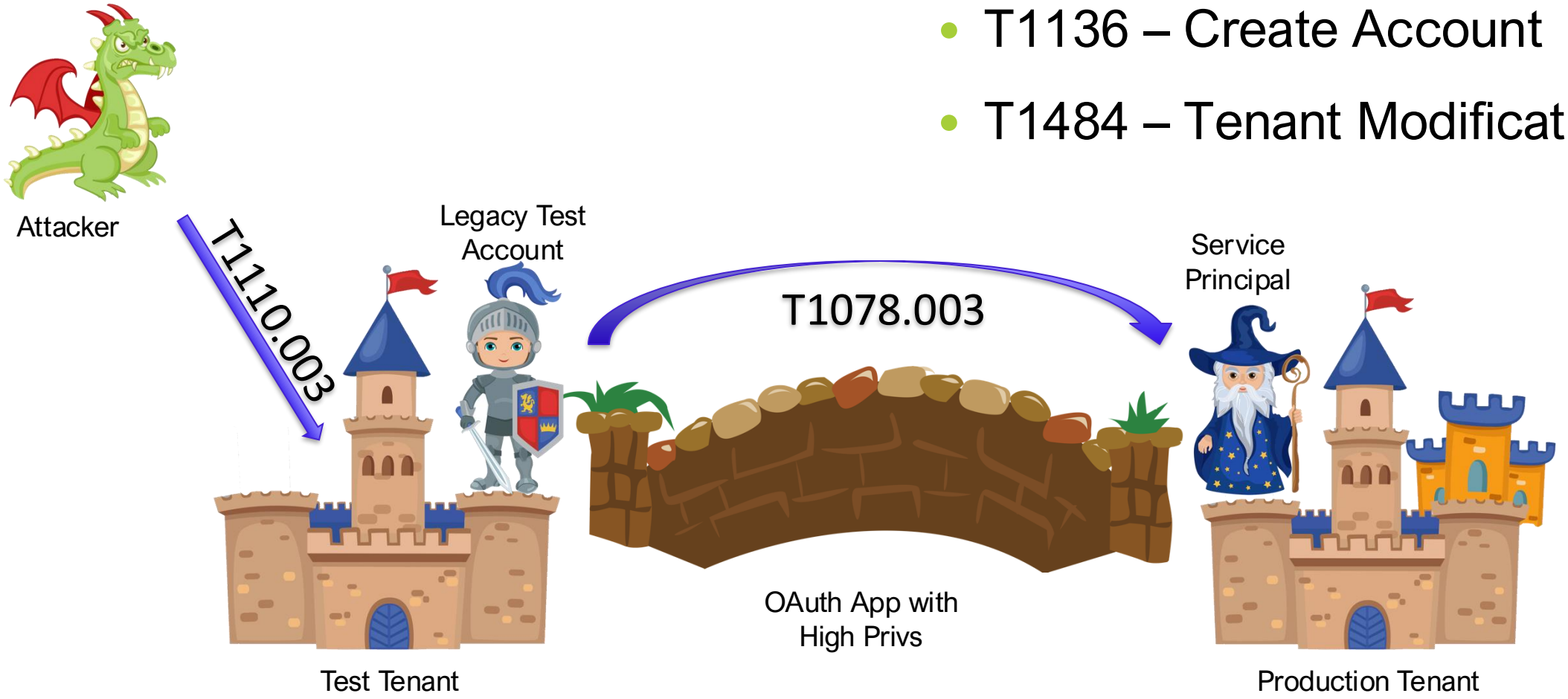
- Full read/write/delete
- Bypasses EntraID
- Contributor=View Key

ON BY DEFAULT!

RSAC 2025 Conference

Betraying Trusts in Azure

- T1110 – Password Spray
- T1078 – Valid Accounts
- T1136 – Create Account
- T1484 – Tenant Modification



RSAC 2025 Conference

Betraying Trusts in Azure

Watch for abandoned/unmanaged infra.

Overly permissive roles are a hard problem.

Audit all trusted relationships between security boundaries.

Initial Access T1199 – Trusted Relationships

Knowing your security boundary

These boundaries occur at various levels, can become apparent as data “crosses” each one.

Customer data ≠ Test data

Internet facing ≠ Internal infrastructure

Production account ≠ Contractor account

Audit and monitor your security boundaries

How to manage security boundaries

- Tools can help: AWS IAM Analyzer, 3rd party software .
- Disable "cross-tenant access" for resources in Azure.
- Regularly audit (by humans) any cross tenant/account IAM resources.
- Enforce ownership – tag all the things.

Architecture, operations, separation of duties must have security boundary enforcement in mind.

What to do on Monday

- Add logging to your security findings/guardrail process.
- MFA all the things.
- Reduce reliance on long term credentials.
- Know your security posture of all deployed resources.
  (If you can't scan it, you can't secure it)
- Audit, alert, investigate your security boundaries.

Start small | Push every day | Measure results

RSAC | 2025 Conference

Many Voices.
One Community.

Shaun McCullough

www.linkedin.com/in/cybergoof

sec541.com/rsa2025